REMARKS

Claims 1, 7-12, 18-22 and 30 are pending in the application and all stand rejected. Reconsideration and allowance of all pending claims is respectfully requested in view of the following:

Responses to Rejections to Claims – 35 U.S.C. §112

Applicant acknowledges and appreciates that the Examiner has withdrawn the previous rejection relating to "key blobs" 224 and 226.

Claims 1, 7-12, 18-22 and 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The rejection reads that "[t]he claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention". In addition, the rejection reads that "[i]ndependent claims 1, 12 and 30 recite 'a session key randomly generated'. However, after careful review of the specification, the examiner finds *no support* in the original specification for a session key that was randomly generated. Emphasis added. This rejection is respectfully traversed.

A written description rejection under 35 U.S.C. §112, first paragraph, places a burden on the USPTO to present a *prima facie* case that the rejected matter does not meet the written description requirement. See MPEP 2163.04. "A written description as filed is presumed to be adequate, unless or until *sufficient evidence or reasoning* to the contrary has been presented by the examiner to rebut the presumption." *Id.* (Citation omitted). "The examiner, therefore must have a reasonable basis to challenge the adequacy of the written description" and *MUST* present "by a preponderance of evidence why a person skilled in the art would *not* recognize in an applicant's disclosure a description of the invention defined by the claims." *Id.* Emphasis added. Applicant submits that the USPTO has failed to present a *prima facie* case under these requirements and the rejection should be withdrawn.

Applicant maintains that argument from the previous response and again points out page 2, lines 7-17 discloses that cryptographic systems commonly use a given set of numbers or digits known as a cipher "key" that may be *randomly chosen* or have special mathematical properties. Emphasis added. Randomly chosen numbers are commonly known in the art as being "generated." Page 7, line 2 discloses that "a session key [is] generated by the system." Additionally, page 11, lines 11-23 discloses that the "second data processing system 204

includes program instructions to generate session key 218." In addition, the Examiner concedes on both page 2 and page 3 of the present Office Action that it is common in the art to generate session keys by a random number. Given that it is common in the art to generate session keys by random number or by other mathematical manipulation, and given that the present application discloses that the session key 218 is generated, surely a person skilled in the art *would* recognize in the disclosure a description of the invention defined by the claims as required by MPEP 2163.04 described above. Therefore, the written description requirement of 35 U.S.C. § 112 is satisfied and withdrawal of this rejection is respectfully requested.

The "Response to Arguments" section on pages 2 and 3 of the present Office Action states that, "[t]he examiner asserts that the independent claims recite three different types of keys (master, public and private). The cited portion of the specification does not specify which of the three keys is randomly chosen or have special mathematical properties [thus, as conceded by the Examiner, it is common in the art to generate keys by random number, therefore, *any of the keys could be randomly generated*]." The Office Action response goes on that "it is also common in the art to generate session keys by passwords. There are multiple ways to generate a session key. So how is the examiner suppose [SP] to know the method of which the applicant is generating a session key. [SP] The examiner asserts that nowhere in the specification does it explicitly recite that a random number generates the session keys." Because it is commonly known to generate any of the keys by random number, it is submitted that surely a person skilled in the art *would* recognize in the disclosure a description of the invention defined by the claims as required by MPEP 2163.04 described above.

In response to Examiner's question of "how is the examiner suppose [SP] to know the method of which the applicant is generating a session key," it is submitted that the claims recite "random" generation of the key. Thus, the claims recite the "method of which the applicant is generating a session key." Therefore, in view of the above, it is again submitted that the written description requirement of 35 U.S.C. § 112 is satisfied and withdrawal of this rejection is respectfully requested.

Responses to Rejections to Claims – 35 U.S.C. §102

Claims 1, 7-8, 12, 18-19 and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Albanese et al (U.S. Patent No. 6,002,768) (Albanese hereinafter). This rejection is not applicable to the amended claims.

Independent claims 1, 12 and 30 all recite, among other things, encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a

public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob.

The USPTO provides in MPEP §2131 that: "[t]o anticipate a claim, the reference must teach every element of the claim."

Therefore, to support the rejections with respect to claims 1, 7, 8, 12, 18, 19 and 30, Albanese must contain all of the elements in the above-mentioned claims. However, Albanese does not disclose encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob.

The Examiner points to column 9, lines 37-43 of Albanese to support his claim that Albanese discloses each of the elements of encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob. However, this section of Albanese reads,

> [i]f the lecture is a private conference session, then the confirmation message additionally includes $\{K_S\}k_{Sn}$, the session key K_S encrypted with a public key provided by the requester in its registration request. Since only the requester knows the corresponding private key (written as k_{nij}^{-1} in the case of a service provider), only the requester will be able to obtain the session key from the confirmation message.

Thus, there is no disclosure or suggestion of *encrypting* the *data* using the *session key* and a *symmetric* encryption routine; *encrypting* the *session key*, with a *public key* of the first user using an *asymmetric* encryption routine, for storage as a first *user key blob*; *encrypting* the *session key*, with a *master public key* using the *asymmetric* encryption routine, for storage as a *master key blob*, as recited in the pending claims. Emphasis added.

Additionally, this section of Albanese discloses that the "*session key* K_s [is] encrypted with a public key", NOT that the session key is *used* to encrypt other data. Thus, all the elements of the pending claims are not found in Albanese. Furthermore, the present Office Action indicates on page 3 that column 6, lines 31-33 of Albanese discloses that "the key for encryption is the same key for decryption" and thus Albanese uses symmetric encryption. However, the pending claims recite using both symmetric and asymmetric encryption routines.

During a quick search of Albanese, neither "symmetric", or "asymmetric" were found. Therefore, Albanese could not disclose, teach, or suggest using one type of encryption over the other. Once again, ALL the elements of the pending claims are NOT found in Albanese. As a result, the previous rejections based on 35 U.S.C. §102(e) cannot be supported by Albanese as applied to claims 1, 12, and 30. Thus, claims 1, 12 and 30 are allowable.

The remaining claims depend from respective ones of the independent claims and are allowable as depending from an allowable independent claim. Therefore, the remaining claims are allowable as depending from an allowable claim. Thus, withdrawal of these rejections is respectfully requested.

Responses to Rejections to Claims – 35 U.S.C. §103

Claims 9, 10, 20 and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese as applied to claims 1 and 12 above, and further in view of Dillaway et al (U.S. Patent No. 5,742,756) (Dillaway hereinafter).

Claims 11 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Albanese as applied to claims 1 and 12 above, and further in view of Kruys (U.S. Patent No. 5,555,309) (Kruys hereinafter). These rejections do not apply to the amended claims for at least the following reason:

Claims 9, 10, 11, 20, 21 and 22 are each dependent claims that depend from either independent claim 1 or 12. As shown above, independent claims 1 and 12 are allowable. Thus, these claims are allowable as depending from an allowable independent claim. Therefore, these rejections are defective and should be withdrawn.

In addition to the previous argument, the PTO recognizes in MPEP §2142:

> The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness.

The examiner clearly cannot establish a *prima facie* case of obviousness in connection with claims 9, 10, 11, 20, 21 and 22 for the following reasons.

35 U.S.C. §103(a) provides that:

> [a] patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains ... (emphasis added)

Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. However, Albanese, Dillaway and Kruys, alone, or in any combination, do not teach a method for encrypting data as claimed. In addition to the shortcomings of Albanese as set forth above, Dillaway teaches in the cited section (Column 3, lines 24-31) a smart card that only holds a private key. However, the smart card discussed on page 10, lines 10-19 of the present application "contains the user's private keys and any public keys, as well as any other data that may be required by the systems with which smart card 134 is utilized." Kruys teaches in the cited section (column 2, lines 56-67) "*public* and *private* key pairs which *share the same key value*." However, the plurality of *private* keys and the plurality of *public* keys claimed in claims 11 and 22 and described on pages 6, line 26 – page 7, line 9 and throughout the application do not have the same key value. For example, with regard to the *public* key, the session key is encrypted twice, once using the *user public* key and once using the *master public* key. Thus, if the plurality of *public keys* were of the same value, there would be no benefit of encrypting the data twice. Additionally, with regard to the plurality of *private* keys, the session key is decrypted using the *user private* key for one user and the session key is decrypted using the *master private* key for a different or third party user. Here again, if the plurality of *private* keys had the same value, there would be no benefit to having the plurality of keys. Therefore, the teaching of Dillaway and Kruys, when combined with the shortcomings of Albanese, do not teach the claimed subject matter as a whole. As a result, it is impossible to render the subject matter of claims 9, 10, 11, 20, 21 and 22 as a whole obvious based on any combination of the patents, and the above explicit terms of the statute cannot be met. As a result, the examiner's burden of factually supporting a *prima facie* case of obviousness clearly cannot be met with respect to claims 9, 10, 11, 20, 21 and 22, and a rejection under 35 U.S.C. §103(a) is not applicable.

There is still another compelling, and mutually exclusive, reason why the references cannot be combined and applied to reject the claims under 35 U.S.C. §103(a).

The PTO also provides in MPEP §2142:

> [T]he Examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the Examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. ...[I]mpermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

Recently, the Supreme Court ruled that the "teaching, suggestion, or motivation (TSM) test" for determining obviousness still applies, but should be used in a more "expansive and flexible" manner. *KSR Int'l. Co. v. Teleflex Inc.*, 550 U.S. __, 11 (2007). The Court stated that "a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known." Id. at 14-15, emphasis added.

In the present case, the Examiner has not expressed a reason why a person of ordinary skill in the art would combine the teachings of Albanese with the teachings of Dillaway as required by claims 9, 10, 20, and 21. Albanese teaches an online conference session management system. Dillaway teaches a smart card that only holds private keys. If the benefits of Albanese are combined with the benefits of Dillaway, as suggested by the Examiner, the result would not combine encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob, which the suggested combination cannot achieve because the suggested combination would result in an online conference session management system having a smart card that only holds private keys.

In addition, the Examiner has not expressed a reason why a person of ordinary skill in the art would combine the teachings of Albanese with the teachings of Kruys as required by claims 11 and 22. Albanese teaches an online conference session management system. Kruys teaches public and private key pairs which share the same key value. If the benefits of Albanese are combined with the benefits of Kruys, as suggested by the Examiner, the result would not be encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob, as is required by

claims 11 and 22. Once again, the pending claims combine encrypting the data using the session key and a symmetric encryption routine; encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob; encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob, which the suggested combination cannot achieve because the suggested combination would result in an online conference session management system where public and private key pairs which share the same key value. Thus, as shown above, if the keys were of the same value, there would be no benefit of encrypting the data twice.

In view of the above, a person of ordinary skill in the art would not have a reason to combine Albanese with either Dillaway or Kruys. Therefore, there is simply no basis for combining the references to support a 35 U.S.C. §103(a) rejection of the claims.

Thus, in the present case it is clear that the USPTO's combination arises solely from hindsight based on the invention without any reason why a person of ordinary skill in the art would combine the references as required by the claims. Therefore, for this mutually exclusive reason, the USPTO's burden of factually supporting a *prima facie* case of obviousness clearly cannot be met with respect to the claims, and the rejection under 35 U.S.C. §103(a) is not applicable.

Therefore, it is impossible to render the subject matter of the claims as a whole obvious based on a single reference or any combination of the references, and the above explicit terms of the statute cannot be met. As a result, the USPTO's burden of factually supporting a *prima facie* case of obviousness clearly cannot be met with respect to the claims, and a rejection under 35 U.S.C. §103(a) is not applicable. Thus, independent claims 1, 12, and 30 and their respective dependent claims are submitted to be allowable.

Conclusion

In view of all of the above, independent claims 1, 12, and 30 and their respective dependent claims are submitted to be allowable. Thus allowance of all currently pending claims is respectfully requested.

The Examiner is invited to call the undersigned at the below-listed telephone number if a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

Bart A. Fisher
Registration No. 55,181

Dated: 6-15-2007

Haynes and Boone, LLP.
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 512.867.8458
Facsimile: 214.200.0853
ipdocketing@haynesboone.com

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office, via EFS-Web, on the date indicated below:

on June 15, 2007
Date

Y. Kim Reyes
Y. Kim Reyes